

REMARKS

In the Office Action, the Examiner rejected Claims 1-22 and 25-44, which are all of the pending claims, under 35 U.S.C. 103 as being unpatentable over the prior art, primarily U.S. Patent 6,453,296 (Iwamura). In particular, Claims 1-5, 7-23 and 26-42 were rejected as being unpatentable over (Iwamura) in view of a document "Introducing Trusted Third Parties to the Mobile Agent Paradigm" (Wilhelml, et al.). Claims 6 and 25 were rejected as being unpatentable over Iwamura in view of Wilhelml, et al. and further in view of U.S. Patent 6,714,982 (McDonough, et al.); and Claims 43 and 44 were rejected as being unpatentable over Iwamura in view of Wilhelml and further in view of U.S. Patent 6,748,528 (Greenfield). The Examiner also noted an informality in Claim 44 and required correction thereof.

Applicants are herein amending independent Claims 1, 31, 33, 34, 37 and 40 to better define the subject matters of these claims. More specifically, features from claim 43 are being added to each of these independent claims. Claim 43 itself is being amended to maintain consistency between the language of Claim 43 and Claim 1, from which Claim 43 depends, and the informality that the Examiner noted in Claim 44 is being corrected.

With respect to Claim 44, the last line of the claim is being amended to correct the spelling of "the," so that this line now reads "...including that the client has properly authenticated." In view of this, the Examiner is asked to reconsider and to withdraw the objection to Claim 44.

In addition, for the reasons set forth below, all of Claims 1-22 and 25-44 patentably distinguish over the prior art and are allowable. The Examiner is thus also asked to reconsider and to withdraw the rejection of Claims 1-22 and 25-44 under 35 U.S.C. 103, and to allow these claims.

As explained in detail in the present application, this invention relates to improving the security of transactions using the world wide web. This is done by enabling a server operator, operating within the existing SSL and Web infrastructure, to provide services with security properties that a remote user can verify. An important feature of the invention is that secure application software, loaded into a trusted co-server, can prove itself – that is, that this is the software running inside the trusted co-server – to arbitrary third parties.

To do this, the co-server application software generates a key pair including a public key and a private key. Then, when a session is established between the client and the co-server application, the client is informed that this co-server application has knowledge of the private key of said key pair.

This feature is clearly not shown in or suggested by either Iwamura or Wilhelm1.

Iwamura describes a special purpose distributed system to support a particular agency's commerce application, and this system uses shared secrets and has the agency distribute secret keys, which make it impossible for the parties involved to prove non-repudiation.

Wilhelm1 discloses a trusted and tamper-resistant hardware device with a manufacture-certified key pair. However, Wilhelm1 uses this key pair to protect a remote shopping agent from malicious behavior.

Each of Independent Claims 1, 31, 33, 34, 37 and 40 describes the above-discussed feature of this invention. In particular, claims 1, 31, 33 and 40 include the step of installing co-server application software in the trusted co-server, where this co-server application software generates a key pair including a public key and a private key. These claims include the further steps of establishing a session between the client and the co-server application, and indicating to the client

that the co-server application demonstrates knowledge of the private key of the key pair.

Claims 34 and 37 describe the features that co-server application software is installed in the trusted co-server and generates a key pair including a private key. These claims also describe the feature that when a session is established between the client and the co-server application, the client is informed that the co-server application has knowledge of the private key of the key pair.

This feature is of significant utility because it helps to provide a universal infrastructure that supports myriad applications from multiple server operators. The invention permits the additional flexibility of allowing the server operator, remote users, server application developers, hardware manufacturers, and SSL CAs all to be separate parties.

This feature of the invention was set forth in Claim 43, and it is believed that the Examiner has recognized that neither Iwamura nor Wilhelm1 discloses this feature. The Examiner, however, argued that Greenfield describes this feature and thus relied on Greenfield, in combination with Iwamura and Wilhelm1, to reject Claims 43 and 44. Greenfield, though, is not prior art as to the present application.

This is so because Greenfield and this application are assigned to the same corporation, IBM Corporation. Applicants submit that the filing of the present application on September 15, 2000, brings the subject application under the rubric of the amendments made to the Patent Law in the American Inventors Protection Act of 1999. That Act, enacted November 29, 1999, amends 35 U.S.C. §103(c) such that subject matter developed by another person which qualifies as prior art under 35 U.S.C. §102(e) does not preclude patentability where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an application of assignment to the same person.

That this section applies to the instant application is established by the Guidelines concerning the implementation of changes to 35 U.S.C. §§102(g) and 103(c) published in the Official Gazette on April 11, 2000. Those Guidelines includes the statement that the amendment to 103(c) applies to all utility, design and plant patent applications filed on or after November 29, 1999, including continuing applications filed under 37 C.F.R. §1.53(d), continued prosecution applications filed under 37 C.F.R. §1.53(b) and reissues. In view of the filing of the present application on September 15, 2000, Applicants benefit from the statutory restraints imposed in the amendment to §103(c).

That the claims of the present application are patentable over the rejection of record is established by the fact that Greenfield is, on its face, assigned to International Business Machines. The instant application is also assigned to International Business Machines. The Assignment of the instant application to International Business Machines by the Applicants of the present application was mailed December 21, 2000, to the USPTO for recording. The Assignment was recorded by the USPTO on December 27, 2000 at Reel 011386, Frame 0421

U.S. Patent 6,748,528 to Greenfield issued June 8, 2004. The present application is entitled to the benefit of the filing date of September 15, 2000. As such, the use of Greenfield to support the rejection of claims of this application is predicated upon availability of Greenfield as a reference under 35 U.S.C. §102(e) in that this is the only subsection of 35 U.S.C. §102 whose requirements are met by this patent.

In view of the requirements of 35 U.S.C. §103(c), as amended November 29, 1999, which apply to the instant application, the Greenfield reference cannot preclude patentability under 35 U.S.C. §103. Thus, Greenfield cannot be applied against Claims 43 or 44, nor can it be applied against Claims 1, 31, 33, 34, 37 and 40 as amended herein.


The other references of record have been reviewed, and these other references, whether considered individually or in combination, also fail to disclose or teach the use of the trusted co-server in the manner described in Claims 1, 31, 33, 34, 37 and 40.

For instance, McDonough does not teach how the users can verify that the server operator is not lying or mistaken when the server operator claims the scanning has been performed.

Because of the above-discussed differences between Claims 1, 31, 33, 34, 37 and 40 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-22, 25-30, 43 and 44 are dependent from Claim 1 and are allowable therewith. Claim 32 is dependent from, and is allowable with, Claim 31; and Claims 35 and 36 are dependent from Claim 34 and are allowable therewith. Further, Claims 38 and 39 are dependent from, and are allowable with Claim 37, and Claims 41 and 42 are dependent from Claim 40 and are allowable therewith.

For the reasons discussed above, the Examiner is asked to reconsider and to withdraw the objection to Claim 44 and the rejections of Claims 1-22 and 25-44 under 35 U.S.C. 103, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,


John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy